

**EXPLANATORY MEMORANDUM TO
THE DATA RETENTION REGULATIONS 2014**

2014 No. 2042

1. This explanatory memorandum has been prepared by the Home Office and is laid before Parliament by Command of Her Majesty.

This memorandum contains information for the Joint Committee on Statutory Instruments.

2. **Purpose of the instrument**

- 2.1 These Regulations are made under the Data Retention and Investigatory Powers Act 2014 (“the Act”). They are intended to revoke and replace the Data Retention (EC Directive) Regulations 2009 (S.I. 2009/859) (“the 2009 Regulations”). They effectively replicate the 2009 Regulations, while providing additional safeguards, in requiring telecommunications service providers to retain certain types of communications data for a period not to exceed 12 months.

3. **Matters of special interest to the Joint Committee on Statutory Instruments**

- 3.1 On 8 April 2014 the European Court of Justice declared the Data Retention Directive (2006/24/EC) (“the Directive”) invalid. The 2009 Regulations implemented the Directive in United Kingdom law. In the light of the Court’s judgment the Act, containing the power to make these Regulations, puts the legal basis for data retention beyond doubt.
- 3.2 The Act was taken through Parliament on a fast-track basis. In order to ensure the new data retention regime is in place before the Summer Recess these Regulations will also be subject to an accelerated Parliamentary timetable. In particular, the Regulations will come into force on the day after they are made. The Government considers it important to put in place a new regime for data retention as soon as possible. This will ensure that telecommunications service providers continue to retain data following the European Court of Justice judgment.
- 3.3 These Regulations effectively replicate the obligations on providers contained in the 2009 Regulations, and do not provide for the retention of any additional categories of communications data. A provider will only be subject to the requirements of these Regulations when it is given a notice by the Secretary of State requiring the retention of data. These Regulations contain transitional provisions for the continued effectiveness of a notice under the 2009 Regulations, until a new notice is given under the new Regulations. These Regulations also contain a requirement to consult a provider before giving a notice. Accordingly, it is not considered that the accelerated timetable and the fact that the Regulations come into force on the day after they are made causes any prejudice to telecommunications providers.

4. Legislative Background

- 4.1 Currently, under the Privacy and Electronic Communications (EC Directive) Regulations 2003 (S.I. 2003/2426), companies are permitted to retain communications data they need for business purposes. Where that data is retained it is available for relevant public bodies to access. However, once the data is no longer needed for business purposes it must be deleted or made anonymous, unless otherwise required by law.
- 4.2 Part 11 of the Anti-Terrorism, Crime and Security Act 2001 (ATCSA) provides a basis for the voluntary retention of communications data in the UK. Parliament approved a voluntary code of practice under that Act in 2003. The Data Retention (EC Directive) Regulations 2007 (S.I. 2007/2199) implemented the Directive in respect of mobile and fixed line telephony. The 2009 Regulations, which revoked and replaced the 2007 Regulations, implemented the Directive with respect to the retention of communications data relating to internet access, internet telephony and internet e-mail as well as mobile and fixed line telephony. These Regulations will revoke and replace the 2009 Regulations.

5. Territorial Extent and Application

- 5.1 This instrument applies to all of the United Kingdom.

6. European Convention on Human Rights

- 6.1 James Brokenshire MP, Minister for Immigration and Security, has made the following statement regarding Human Rights:

“In my view the provisions of the Data Retention Regulations 2014 are compatible with the Convention rights.”

7. Policy background – what is being done and why

- 7.1 Communications data is the context not the content of a communication. It can be used to demonstrate who was communicating; when; from where; and with whom. It can include the time and duration of a communication, the number or email address of the originator and recipient, and sometimes the location of the device from which the communication was made. It does not include the content of any communication: for example the text of an email or a conversation on a telephone. Communications data is used by the intelligence and law enforcement agencies during investigations regarding national security and, organised and serious crime. It enables investigators to identify members of a criminal network, place them in specific locations at given times and in certain cases to understand the criminality in which they are engaged. Communications data can be vital in a wide range of threat to life investigations, including the investigation of missing persons. Communications data can be used as evidence in court.

- 7.2 Communications data policy can broadly be split into two policy areas: retention and acquisition. If data is not retained it cannot be accessed. Considering its importance to law enforcement and the security service, it is crucial to ensure it is retained and can be accessed by relevant public authorities under strict controls.
- 7.3 Mandated retention of communications data is currently covered by the 2009 Regulations, which provided for telecommunications providers that have been issued a notice by the Secretary of State to retain specified data for a period of 12 months. Without mandatory data retention relevant public authorities would still be able to access data retained under the voluntary code or for business purposes. However, this is not a substitute for the 2009 Regulations. Many companies are not signed up to the voluntary code and certain types of data may only be retained for a matter of days. Much of the data retained for business purposes would be deleted after only a few months, rather than the 12 months required by the 2009 Regulations. A 2012 Association of Chief Police Officers survey demonstrated that many investigations require data that is older than the few months that data may be retained for business purposes, particularly in ongoing investigations into offences such as child abuse and financial crime.
- 7.4 These Regulations only differ from the 2009 Regulations in that they provide additional safeguards. They provide for data to be retained for a maximum of 12 months, allowing different data types to be retained for shorter periods when appropriate. The 2009 Regulations provided for a blanket 12 months, while the Directive, on which they were based, allowed for between 6 and 24 months. These Regulations also provide for a number of issues the Secretary of State must consider before issuing a retention notice, including taking reasonable steps to consult the provider affected. While this has occurred in the past, the intention is to enshrine best practice in law. Significantly, these Regulations reproduce the Schedule to the 2009 Regulations in respect of the types of communications data that can be retained under a notice. No additional data types will be permitted to be retained under these Regulations than could be retained under the 2009 Regulations.
- 7.5 These Regulations also include transitional provisions. This is to ensure that data that is currently retained under the 2009 Regulations will continue to be retained under these new Regulations. However, it is made clear that the retention period in respect of data that has already been retained under the previous regime does not start again.

8. Consultation outcome

- 8.1 The 2009 Regulations, which these Regulations broadly replicate, were subject to a 12 week public consultation exercise which concluded in October 2008. During that exercise, Home Office officials met with a broad range of public communications providers and their trade associations, the Association of Chief Police Officers, the intelligence agencies, privacy lobbyists and other individuals. A total of 54 responses were received.
- 8.2 Due to the pressing nature of this legislation only a limited process of consultation has been completed with those affected by the provisions, including the communications industry, and law enforcement and intelligence agencies. Many of these stakeholders

have expressed a desire for clarity as to the legal status of data retention. These Regulations and the Act provide that clarity.

9. Guidance

- 9.1 These Regulations make provision for a statutory code of practice in order to provide detailed guidelines for data retention and information about the application of safeguards.

10. Impact

- 10.1 The impact on business, charities or voluntary bodies is cost neutral.
- 10.2 The impact on the public sector is cost neutral.
- 10.3 An Impact Assessment was published during the passage of the Bill through Parliament. This covered both the impact of the Bill and regulations made under the Bill. It is attached here for convenience.

11. Regulating small business

- 11.1 The legislation applies to small business.
- 11.2 The 2009 Regulations had sufficient measures to mitigate the impact on businesses employing up to 20 people. These Regulations reproduce and extend those safeguards. Firms will only be required to retain data if the Secretary of State issues a notice to them requiring them to do so. There is the additional safeguard that the Secretary of State will be required to formally consider the impact on the telecommunications service operators before issuing a notice. As in the 2009 Regulations, all telecommunications companies which incur additional costs as a result of the Regulations will be reimbursed.

12. Monitoring & review

- 12.1 The Act has a sunset clause of 31 December 2016. This is to ensure that debates over communications data policy continue and legislation is revisited in the next Parliament.

13. Contact

- 13.1 Henry Hirsch at the Home Office, Tel: 020 7035 6798 or email: henry.hirsch@homeoffice.x.gsi.gov.uk, can answer any queries regarding this instrument.